ABSTRACT OF THE DISCLOSURE

A method and apparatus for selectively enforcing network security policy using group identifiers are disclosed. One or more access controls are created and stored in a policy enforcement point that controls access to the network, wherein each of the access controls specifies that a named group is allowed access to a particular resource. A binding of a network address to an authenticated user of a client, for which the policy enforcement point controls access to the network, is created and stored. The named group is updated to include the network address of the authenticated user at the policy enforcement point. A packet flow originating from the network address is permitted to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network. Accordingly, network security may be implemented in the form of abstract groups that include specific network addresses; as a result, users may be allowed or denied access to network addresses by updating membership of the groups to include or delete the network addresses of the users, rather than by creating or deleting access controls that specifically identify the users.